Cybersecurity OT&E – Guidance

General Guidance

The body of the TEMP should illustrate that cybersecurity (formerly called Information Assurance) is fully integrated into the developmental and operational test strategies. As needed, provide details on the cybersecurity test and evaluation strategy in Appendix E.

Operational Test Agencies (OTAs) will include cyber threats among the threats to be encountered in operational testing of DOT&E oversight systems with the same rigor as other threats. The purpose of cybersecurity operational testing is to evaluate the ability of a unit equipped with the system to support assigned missions in the expected operational environment.

The system is considered to encompass hardware, software, user operators, maintainers, and the training and Tactics, Techniques, and Procedures (TTPs) used to carry out the Concept of Operations. The operational environment includes other systems that exchange information with the system under test; that is, the system under test is considered a system-of-systems to include the network environment, end users, administrators, cyber defenders, and cyber threats.

In the memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (1 August 2014), henceforth referred to as DOT&E 2014, DOT&E requires a two-phase approach for operational cybersecurity testing. The first phase is called the Cooperative Vulnerability and Penetration Assessment (CVPA). A CVPA is an overt and cooperative examination of the system to identify all significant cyber vulnerabilities and the level of capability required to exploit those vulnerabilities. CVPAs are conducted in the intended operational environment with representative system operators, system/network administrators, and local cyber defenders present to assist the test team in their evaluation. This testing may be integrated with Developmental Test and Evaluation (DT&E) activities if: (1) the event is conducted in a realistic operational environment, (2) the test plan is approved by DOT&E in advance, and (3) the test data is provided to DOT&E. The OTA will include the Program Office in CVPA activities so that the Program Office can learn about any cybersecurity vulnerabilities and how to mitigate them prior to the second phase of operational cybersecurity testing, the Adversarial Assessment.

The Adversarial Assessment (AA) gauges the ability of a system to support its mission(s) while withstanding validated and representative cyber threat activity. Because time and resource constraints prevent representing higher-level threat capabilities in an operational test, the AA phase should use the report generated from the CVPA as input. The AA shall evaluate the ability to protect the system/data, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity; these capabilities are collectively referred to as PDRR – Protect, Detect, React, and Restore. The AA will also assess the effect on the system's missions through direct measurement or by a well-defined methodology using expert input. To provide operational realism and comprehensive PDRR data collection, both local and non-local (e.g., Tier 2) network defenders should participate during the AA. Systems which include continuity of operations (COOP) in their Concept of Operations should include a COOP

demonstration as part of the Restore evaluation. The AA should be conducted in concert with other operational testing, but might require dedicated test time or assets that do not compete for time or resources with other operational test objectives. A CVPA and AA will normally be required as part of any operational test or assessment that supports a fielding decision.

For information systems that manage financial/fiscal/business activities or funds, OTAs should assess the security and resilience of mission-essential logistic and business-focused systems. A Cyber Economic Vulnerability Assessment (CEVA) shall include the development and execution of exploitation scenarios (Cyber Economic Threat Analysis & Cyber Economic Scenario Testing) and a review of financial transactions for evidence of fraud (Financial Transaction Analysis). When appropriate, the CEVA may be conducted in conjunction with the AA. For more information about CEVA systems, see the DOT&E memorandum, "Cyber Economic Vulnerability Assessments (CEVA)" dated January 21, 2015.

Cybersecurity Information for the Body of the TEMP

The cybersecurity OT&E strategy should be integrated into the body of the TEMP in the following paragraphs:

- Paragraph 1.3. System Description. Describe the operational configuration and environment in which the system will operate. Discuss the cybersecurity of the system from an operational perspective. Specify the system users (e.g., unit), the personnel that administer/maintain the system, the local and any non-local (e.g., Tier 2 Computer Network Defense Service Provider[1]) cyber defenders. Identify the known potential cyber attack pathways. (TEMP Body Example)
- Paragraph 1.3.4. System Threat Assessment. Describe the threat environment in which the system will operate, including potential cyber threats (e.g., nearsider), modes of attack (e.g., malware via USB port on maintenance laptop), and objectives (e.g., on-demand weapon failure). Reference the most recent Defense Intelligence Agency (DIA) Computer Network Operations Capstone Threat Assessment or component-validated threat documents for the system. (TEMP Body Example)
- Paragraph 2.5. Integrated Test Program Schedule. Show the CVPA and AA test events on the Integrated Program Test Schedule (Figure 2.1).
- Paragraph 3.3.2. Developmental Test Events. For systems that are mature enough to participate in a realistic network environment in an operationally-representative configuration, programs may integrate CVPAs into the developmental phase of testing. If so planned, identify when and where the CVPAs will be conducted, which OTA will conduct the CVPA, and ensure DOT&E approval of the CVPA plan.

---

1 The DoD has elevated many cyber defense functions from the unit level to Service and DoD Agency Computer Network Defense Service Providers (CNDSPs, sometimes also called Cybersecurity Defense Service Providers) supporting large geographic regions, such as Combatant Command areas of responsibility or even globally. Every system is required by DoD policy to interoperate one of these providers unless specifically exempted. If a system does not interoperate with a CNDSP, the TEMP should so state.

- Paragraph 3.5. Operational Evaluation Approach. Describe the overall strategy for evaluation of cybersecurity in support of mission accomplishment, suitability, and survivability. Define cybersecurity measures for Protect, Detect, React, and Restore. (TEMP Body Example)
- Paragraph 3.5.1 Operational Test Events and Objectives. Identify when the CVPAs, AAs, and CEVAs (if required) will be conducted, noting that CVPAs must necessarily (1) precede AAs,[2] (2) be of sufficient duration to identify all significant vulnerabilities and (3) provide the adversarial team with enough data to portray a realistic threat. For each test, include a cybersecurity test architecture with test boundary identifying which systems are to be included and excluded from each test. If not provided elsewhere in the TEMP, define the cybersecurity critical issues and measures. (TEMP Body Example)
- Paragraph 3.5.1.1 Cooperative Vulnerability and Penetration Assessment. Define the data collection methods, which may include automated scanning/exploitation tools, physical inspection, document reviews, and personnel interviews. Identify all data and metrics to be collected, to include, at minimum, those listed in Attachments A and B of DOT&E 2014. Specify the independent cyber team that will execute the CVPA cyber activities for the OTA. State how far in advance the adversarial team will be provided access to the CVPA team's report and data. (TEMP Body Example)
- Paragraph 3.5.1.2 Adversarial Assessment. Identify the NSA-certified and USCYBERCOM-accredited team that will execute the AA cyber activities for the OTA. Identify the team responsible for collecting, at a minimum, the Protect, Detect, React, and Restore (PDRR) data specified in Attachment C of DOT&E 2014 from both local and non-local (e.g., Tier 2) cyber defenders. Specify the duration of the assessment; ideally, the engagement is long enough to represent a realistic threat (e.g., a so-called advanced persistent threat). Document the intelligence community-recognized cyber threat and specify whether the mission effects of the adversarial attack will be assessed by direct measurement of the effect on system performance parameters (e.g., rounds per minute) or an assessment by independent subject matter experts. Specify who will act as the local and higher-tier cyber defenders to provide Detect and React data; the OTA may need additional data collectors to collect the Detect and React data. If intrusion detections are not made, state that the React and Restore data will be collected using white cards. If subject matter experts will assess the mission effects, briefly describe their proposed methodology. (TEMP Body Example)
- Paragraph 3.5.1.3 Cyber Economic Vulnerability Assessment. (If required) Identify the test teams that will support the CEVA; this should include an NSA-certified and USSCYBERCOM-accredited cyber team and an accounting firm. Name the system

[2] Ideally, the CVPA will be far enough advance of the AA to allow the program office to mitigate any vulnerabilities discovered in the CVPA prior to the AA.

and economic subject matter experts who will assist in the Cyber Economic Threat Analysis and assess the mission effects of exploitation, and provide some discussion of their qualifications for these roles. Cyber Economic Vulnerability Assessments (CEVA).

- Paragraph 3.5.1.4. Cybersecurity Test Architecture. Include a detailed diagram indicating which of the following elements are included (inside the test boundary) or excluded from the test: (TEMP Body Example)
  - Major sub-systems (e.g., guidance and communication)
  - All connections between the subsystems including their protocols (e.g., target identification receives input from both Link 16 and the fire control radar via a 1553 data bus)
  - All external connections, direct (e.g., CENTCOM via NIPRNet, SIPRNet, or JWICS) or indirect (e.g., maintenance laptop, Mission Planning System data transfer devices)
  - All physical access points (e.g., operator consoles) and removable media ports (e.g., USB ports, CD/DVD drives)
- All other systems to which the system will connect (e.g., SATCOM) (TEMP Body Example)
- Paragraph 3.5.2.1. Cybersecurity Critical Issues. Identify the critical issues affected by cybersecurity and describe the cybersecurity evaluation criteria for each test. (TEMP Body Example)
- Paragraph 3.5.4 Test Limitations. Identify any restrictions that may affect the efficacy or realism of the planned CVPA, AA, or CEVA (e.g., adversarial team not allowed to alter data on the system) and any associated mitigations (e.g., white cards, validated laboratory environment). (TEMP Body Example)
- Paragraph 4.2.5 Resources for Cybersecurity Threat. For each CVPA, AA, and CEVA (if required), specify the allocation of operational and cyber defense resources for the system. Outline the funding requirements for operational cybersecurity testing and test team manpower requirements. Identify any external organizations (and associated resources) required to participate in testing. Also specify resources for developing cyber exploitation tools or techniques that the CVPA and AA cyber teams do not already possess (e.g., developing malicious software images for embedded systems). (TEMP Body Example)

Cybersecurity OT&E Information for Appendix E

Details about the cybersecurity OT&E strategy should be included in Appendix E if not already stated in the body of the TEMP. If cybersecurity is completely described in the body of the TEMP, a cybersecurity appendix is not required.

Examples

TEMP Main Body Example for Tactical Ground Vehicle System

Appendix E Example for Shipboard System

Appendix E Example for Command and Control System

Appendix E Example for Tactical Aircraft System

References

Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, DOT&E, 1 August 2014

Cyber Economic Vulnerability Assessments (CEVA), DOT&E, 21 January 2015

Cybersecurity Test and Evaluation Guidebook, DoD, 1 July 2015